

AO 106 (Rev. 04/10) Application for a Search Warrant

## UNITED STATES DISTRICT COURT

for the  
Southern District of California

FILED

AUG 16 2019

CLERK US DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA  
BY \_\_\_\_\_ DEPUTY

In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*THE RESIDENCE OF TRORICE CRAWFORD  
LOCATED AT 4078 34TH STREET,  
SAN DIEGO, CA 92104

Case No.

19MJ3464

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, which is incorporated by reference.

located in the Southern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is incorporated by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

*Code Section*  
18 U.S.C. §§ 1343, 1349,  
1956, 1028A

*Offense Description*  
Wire fraud; conspiracy to commit wire fraud; conspiracy to commit money  
laundering; and aggravated identity theft.

The application is based on these facts:

See Affidavit of Department of Defense Special Agent Jacob W. Dye, which is hereby incorporated by reference and made part hereof.

- ☒ Continued on the attached sheet.
- ☒ Delayed notice of 30 days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

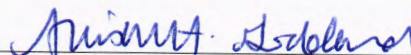


Applicant's signature

JACOB DYE, Special Agent, DCIS

Printed name and title

Sworn to before me and signed in my presence.

Date: 8/16/19


Judge's signature

City and state: San Diego, California

Hon. Allison Goddard, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF CALIFORNIA

IN THE MATTER OF  
THE SEARCH OF:

THE RESIDENCE OF  
TRORICE CRAWFORD  
LOCATED AT  
4078 34<sup>TH</sup> STREET,  
SAN DIEGO, CA 92104

Case No. \_\_\_\_\_

~~Filed Under Seal~~ JWD

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Jacob Dye, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent with the Department of Defense, Office of the Inspector General, Defense Criminal Investigative Service (DCIS), assigned to the Cyber West Resident Agency in San Diego, California. I have served in this capacity for three years. Prior to my current employment with DCIS, I served as a Special Agent with the United States Secret Service, Homeland Security Investigations, and the U.S. Army Criminal Investigation Command for a total of eighteen years. While assigned to the DCIS Cyber West Resident Agency, I have been designated to investigate cybercrimes and computer networks, which includes crimes involving the compromise and theft of sensitive defense information contained in government and contractor information systems. Additional duties include providing digital exploitation and forensics services in support of traditional investigations. I also have experience conducting investigations involving the following: national security threats; computer compromises; financial crimes; and commercial fraud. During the course of my duties, I have been involved in the execution of search warrants conducted on

1 businesses, email accounts and homes, which have included the search of computers and  
2 associated media storage devices.

3 2. I am a graduate of the Criminal Investigator Training Program taught at the  
4 Federal Law Enforcement Training Center (FLETC), located at Glynco, Georgia. I am also  
5 a graduate of the DCIS Special Agent Training Program, the ICE Special Agent Training  
6 Academy, and the U.S. Secret Service Special Agent Training Program. Additionally, I have  
7 attended the Introduction to Computers and Hardware, Cyber Threats and Techniques,  
8 Network Intrusion Basics, Computer Incident Responders, Windows Forensic Examination,  
9 and the Forensic Intrusion in a Network Environment courses at the Defense Computer  
10 Investigative Training Academy, Linthicum, Maryland. I am a certified as a Digital Evidence  
11 Collector, Digital Forensic Examiner, and Defense Cyber Investigator. I have also attended  
12 workshops related to forensic telephone recovery, use of telephone data in investigations, and  
13 GPS data exploitation.

14 3. On July 23, 2019, a federal grand jury in the Western District of Texas returned  
15 a sealed indictment charging Robert Boling, Jr. (BOLING), Fredrick Brown (BROWN),  
16 Trorice Crawford (CRAWFORD), and others with violating 18 U.S.C. §§ 1343 (wire fraud),  
17 1349 (conspiracy to commit wire fraud), 1956 (conspiracy to commit money laundering) and  
18 1028A (aggravated identity theft) (collectively, the SUBJECT OFFENSES). That indictment  
19 is attached as Exhibit 1 to this Affidavit. Arrest warrants for the indicted individuals were  
20 also issued on the same day. On or about August 6, 2019, BOLING and one of the other  
21 individuals who was also indicted were arrested in the Philippines. On or about August 13,  
22 2019, BROWN was arrested in Las Vegas, Nevada.

23 4. I make this affidavit in support of an application under Federal Rule of  
24 Criminal Procedure 41 for a warrant to search CRAWFORD's residence located at 4078 34<sup>th</sup>

1 Street, San Diego, CA 92104 (hereinafter SUBJECT PREMISES), which is further described  
2 in Attachment A, for the things described in Attachment B.

3 5. Based on the facts set forth in this affidavit, there is probable cause to believe  
4 that BOLING, BROWN, and CRAWFORD have committed the SUBJECT OFFENSES  
5 and that the SUBJECT PREMISES will contain evidence of the SUBJECT OFFENSES. As  
6 such, there is also probable cause to search the SUBJECT PREMISES described in  
7 Attachment A for evidence of these crimes, contraband and/or fruits of these crimes, as  
8 described in Attachment B.

9 6. The facts set forth in this affidavit are based upon my personal knowledge, my  
10 training and experience, observations, and information obtained from other agents and/or  
11 witnesses. This affidavit is intended to show only that there is sufficient probable cause for the  
12 requested warrant and does not set forth all of my knowledge about this matter.

### 13 TECHNICAL DEFINITIONS

14 7. Based on my training and experience, I use the following technical terms to  
15 convey the following meanings:

16 a. IP Address: The Internet Protocol address (or simply "IP address") is a  
17 unique numeric or alphanumeric address used by computers on the Internet. An IP version 4  
18 address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g.,  
19 121.56.97.178). An IP version 6 address contains 128 bits each and appears as a hexadecimal  
20 digit (meaning it can use 0-10 plus 'a' through 'f') separated by colons (e.g.,  
21 fe80::d4a8:6435:d2d8:d9f3b11). Every computer attached to the Internet must be assigned an  
22 IP address so that Internet traffic sent from and directed to that computer may be directed  
23 properly from its source to its destination. Most Internet service providers control a range of  
24



1 IP addresses. Some computers have static—that is, long-term—IP addresses, while other  
2 computers have dynamic—that is, frequently changed—IP addresses.

3           b. Internet: The Internet is a global network of computers and other  
4 electronic devices that communicate with each other. Due to the structure of the Internet,  
5 connections between devices on the Internet often cross state and international borders, even  
6 when the devices communicating with each other are in the same state.

7           c. Storage medium: A storage medium is any physical object upon which  
8 computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash  
9 memory, CD-ROMs, and other magnetic or optical media.

10           d. Digital device: Computers, computer tablets (e.g. Ipads), electronic  
11 storage devices (e.g., hard drives, thumb drives), and mobile phones.

12           8. Further, as used herein, the terms “records,” “documents,” “programs,”  
13 “applications,” and “materials” include records, documents, programs, applications, and  
14 materials created, modified, or stored in any form, including in digital form on any digital  
15 device and any forensic copies thereof.

16           **TRAINING AND EXPERIENCE REGARDING DIGITAL DEVICES**

17           9. Based on my training, my experience, and my discussions with other law  
18 enforcement agents, I know the following.

19           10. Users of digital devices increasingly choose to store items in digital form (e.g.,  
20 pictures, documents) because digital data takes up less physical space and can be easily  
21 organized and searched. Users also choose to store data in their digital devices because it is  
22 more convenient for them to access data in devices they own, rather than to later spend time  
23 searching for it. Keeping things in digital form can be safer because data can be easily copied  
24 and stored off-site as a failsafe.

1           11. Users also increasingly store things in digital form because storage continues to  
2 become less expensive. Today, 500 gigabyte (GB) hard drives are not uncommon in  
3 computers. As a general rule, users with 1 gigabyte of storage space can store the equivalent  
4 of 500,000 double-spaced pages of text. Thus, a 500 GB computer can easily contain the  
5 equivalent of 250 million pages, that, if printed out, would fill three 35' x 35' x 10' rooms.  
6 Similarly, a 500 GB drive could contain 450 full run movies, or 450,000 songs, or two million  
7 images. With digital devices, users can store data for years at little or no cost.

8           12. Given the capacity and increased use of storage media, there is probable cause  
9 to believe that things that were once stored on a digital device may still be stored there.

10          13. Forensic review of a digital device can also indicate who has used or controlled  
11 the device.

12          14. A person with appropriate familiarity with how an electronic device works  
13 may, after examining this forensic evidence in its proper context, be able to draw conclusions  
14 about how electronic devices were used, the purpose of their use, who used them, and when.

15          15. As further described below, and in Attachment B, this application seeks  
16 permission to locate not only electronically stored information that might serve as direct  
17 evidence of the SUBJECT OFFENSES, but also forensic evidence that establishes how the  
18 device was used, the purpose of its use, who used it, and when. Based on the above, there is  
19 probable cause to believe that this forensic electronic evidence might be on digital devices  
20 located at the SUBJECT PREMISES.

21          16. Pursuant to Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am  
22 applying for would permit the examination of the device consistent with the warrant. The  
23 examination may require authorities to employ techniques, including but not limited to  
24

1 computer assisted scans of the entire medium, that might expose many parts of the device to  
2 human inspection in order to determine whether it is evidence described by the warrant.

### 3 BACKGROUND ON INVESTIGATION

4 17. The United States, including DCIS and the Consumer Protection Branch  
5 (CPB) of the Department of Justice, is investigating BOLING, BROWN, CRAWFORD, and  
6 others for their involvement in an identity theft scheme targeting victims with a military  
7 association<sup>1</sup> (hereafter “military-affiliated individuals”). The investigation has revealed that  
8 the ringleader of the scheme, BOLING is based in the Philippines, with co-conspirators  
9 throughout the Philippines and the United States. BROWN and CRAWFORD are two of  
10 BOLING’s primary co-conspirators.

11 18. Around November 20, 2017, a loss prevention analyst (“LPA”) for the Army  
12 and Air Force Exchange Service (“AAFES”)<sup>2</sup> alerted DCIS agents to apparent fraud  
13 associated with numerous “MilStar” accounts.<sup>3</sup> AAFES issues credits cards – called MilStar  
14 credit cards – to military-affiliated individuals. The AAFES LPA identified a suspicious  
15 pattern of online MilStar accounts being created and subsequently used to make travel-related  
16 purchases tied to the Philippines and Indonesia. Some of the newly-created online MilStar  
17 accounts appeared to use the personal identifiers of actual MilStar customers who did not  
18 themselves have active online MilStar accounts, and other online accounts were created using  
19 personal identifiers of MilStar-eligible service members and military family members who did

---

20  
21 <sup>1</sup> *I.e.*, those on active duty, reservists, retired service members, military spouses, and military dependents.

22 <sup>2</sup> “AAFES” is an entity under the Department of Defense which sells basic consumer goods to service members, retirees, and their dependents at Army and Air Force installations.

23 <sup>3</sup> MilStar credit cards can be used both in-person at AAFES facilities and online through AAFES’ merchant website, [www.shopmyexchange.com](http://www.shopmyexchange.com). AAFES also runs the Exchange Credit Program (“ECP”), which is the rewards program for MilStar credit cards, accessible  
24 online at the domain [www.myecp.com](http://www.myecp.com).

1 not have MilStar accounts. Records obtained from the AAFES LPA revealed that at least  
2 eighty (80) fraudulent MilStar accounts were created using stolen personally-identifying  
3 information (PII) from military-affiliated individuals.

4 19. DCIS and CPB subsequently opened an investigation into the above-referenced  
5 fraudulent activity, which resulted in the collection of substantial amounts of evidence  
6 produced in response to warrants and subpoenas to various companies, including Cox  
7 Communications, Google, Microsoft, Facebook, Dropbox, Metro PCS/T-Mobile, and  
8 multiple financial institutions. A review of these seized materials, led to the identification of  
9 BOLING as the principal orchestrator of an extensive identity theft scheme involving  
10 military-affiliated individuals. As set forth below, BOLING coordinated with his high school  
11 classmate BROWN to steal PII of military-affiliated individuals. BOLING further  
12 coordinated with CRAWFORD in exploiting the stolen PII to steal money from military-  
13 affiliated individuals, government-benefit programs, and financial institutions and remit the  
14 stolen money to co-conspirators located in the Philippines.

15 20. As further explained below, records indicate that the SUBJECT PREMISES at  
16 issue in this warrant is CRAWFORD's current address.

17 **PROBABLE CAUSE**

18 21. The investigation revealed that BROWN was the primary source of stolen PII,  
19 as follows:

20 a. While employed with the U.S. Army as a civilian medical records  
21 technician from 2010 through September 2015 at Yongsan Garrison in South Korea,  
22 BROWN worked with a database called the Armed Forces Health Longitudinal Technology  
23 Application ("AHLTA"). In addition to other PII, AHLTA contained the name, social  
24



1 security number, Department of Defense ID number, date of birth, gender, mailing address,  
2 and telephone number of military-affiliated individuals.

3 b. During the course of his employment, BROWN – who had access to the  
4 PII of thousands of military-affiliated individuals – began taking digital photographs of the  
5 PII and transmitting the stolen information to BOLING. The metadata for these photos show  
6 that BROWN started taking pictures of his AHLTA screen as early as July 2014. Investigation  
7 revealed that BROWN and BOLING referred to these pictures of PII as “lists.”

8 c. I have also reviewed the contents of Dropbox accounts (obtained through  
9 search warrants) associated with one of the co-conspirators linked to this case.<sup>4</sup> In addition to  
10 photos of the co-conspirators and their families, these Dropbox accounts contained photos of  
11 PII of more than 3,300 military-affiliated individuals. The photos depict PII as it appears on  
12 a computer screen when retrieved through AHLTA.

13 22. I have reviewed the records provided by Facebook in response to two 2015  
14 search warrants. I have also reviewed recent records produced by Facebook in response to a  
15 search warrant issued on June 18, 2019. BOLING and BROWN<sup>5</sup> communicated about the  
16 scheme using Facebook Messenger, a private instant-messaging app and platform linked to  
17 the social media website Facebook, for example:

18  
19  
20 <sup>4</sup> Pursuant to a Dropbox search warrant issued on January 22, 2019, agents searched  
21 multiple accounts linked to Jongmin Seok (SEOK) – who was indicted for his involvement  
22 in this identity theft conspiracy along with BOLING, BROWN, and CRAWFORD on July  
23 23, 2019.

24 <sup>5</sup> BROWN used a Facebook account under the name FREDRICK BROWN. The profile  
picture for this account shows a photo of BROWN. Through previous search warrants and  
subpoenas, the investigation has also revealed that BROWN uses the email address  
[brown.fredrick@gmail.com](mailto:brown.fredrick@gmail.com).

1           a. On February 17, 2015, BOLING<sup>6</sup> contacted BROWN using Facebook  
2 Messenger to advise that he had two Western Union transactions that were ready to be sent.  
3 He further stated that he wishes that there was a place “on base” to perform such a transaction,  
4 but worries that someone would get in trouble if it was done on base. BROWN then asked if  
5 there were any specific names that BOLING would like to use, and BOLING responded that  
6 he would take any name.

7           b. On April 17, 2015, BOLING asked BROWN for “Filipino names”  
8 instead of “white names.” BROWN then tells BOLING that he wants a bigger cut if he does  
9 this for BOLING. BOLING agrees but tells BROWN to “make them good.”

10           c. In another Facebook Messenger exchange in April 2015, BOLING asked  
11 BROWN “U got some lists?” to which BROWN replied “Hell Yea. Ima get lists soon as I  
12 scoop it.”

13           d. In a more recent exchange on Facebook Messenger on November 18,  
14 2017, BOLING told BROWN: “But I really COULD use some lists this weekend so I ain’t  
15 gotta start from these crumbs again lmao.” BROWN replied: “Ima get u some soon.”

16           e. And as recently as, April 12, 2018, BOLING again messaged BROWN  
17 via Facebook Messenger stating that he “Could use some lists...”

18           23. As noted previously, the investigation further revealed that BOLING was the  
19 principal orchestrator of this identity theft scheme. BOLING received the stolen PII from  
20 BROWN and, armed with this information, he recruited a network of individuals with whom  
21 he coordinated and/or directed to exploit the stolen PII in order to commit identify theft; and  
22 steal money from military-affiliated individuals, government-benefit programs, and financial

23 \_\_\_\_\_  
24 <sup>6</sup> Investigation revealed that during this time and to the present, BOLING was living in the  
Philippines.

1 institutions. Through the use of individuals in the U.S. who provided their bank accounts to  
2 receive stolen funds (“money mules”), BOLING orchestrated remittance of the fraudulently  
3 acquired funds from the United States to himself and other co-conspirators located in the  
4 Philippines.

5 a. BOLING used two Facebook accounts: one account under the name  
6 LIESURE SUIT LARRY (Facebook ID 100009640415140); and a second account that, in  
7 2015, used the name WAYNE BOLING (BOLING’s middle name is Wayne), but now uses  
8 the name ALFREDO REYES (Facebook ID 100008547813099). Publicly available profile  
9 pictures for both of those accounts show a photo of BOLING.

10 b. Additionally, through previous search warrants, subpoenas, and other  
11 investigatory methods, the investigation also revealed that BOLING uses the following email  
12 addresses: ctm1172@gmail.com, bolingjunior@gmail.com, and  
13 wayneboling0600@gmail.com. Ctm1172@gmail.com is one of the email addresses  
14 associated with both of BOLING’s Facebook accounts between 2015 to present.

15 24. Additionally, the investigation revealed that CRAWFORD, a U.S. citizen,  
16 served as BOLING’s recruiter and supervisor of the “money mules” located in the vicinity of  
17 San Diego, California. CRAWFORD coordinated with BOLING to deposit funds stolen  
18 from military-affiliated individuals into money mules’ accounts, and assisted in remitting  
19 stolen funds from money mules’ accounts to BOLING and other members of the conspiracy  
20 in the Philippines.

21 a. CRAWFORD used two Facebook accounts – one under the name  
22 TRORICE CRAWFORD (FACEBOOK ID: 100000635605550) and the other under the  
23 name SPRINGVALLEY SAYDAT (FACEBOOK ID: 100007172643822). The profile  
24 picture for these accounts display a photo of CRAWFORD.

1           b. Facebook records provided in response to a search warrant issued on  
2 June 18, 2019, show that 619-372-5591 is the cell number associated with the Facebook  
3 account registered to SPRINGVALLEY SAYDAT. Records provided in July 2019 by Metro  
4 PCS/T-Mobile also identify CRAWFORD as the subscriber for the cellular device with  
5 assigned number 619-372-5591.

6           c. As of July 10, 2019 cashmirepurple@gmail.com is the registered contact  
7 e-mail address associated with SPRINGVALLEY SAYDAT. This email address was also  
8 previously associated with the Facebook account under the name TRORICE CRAWFORD.  
9 At present, Fastcask2k10@aol.com is the registered email address associated with the  
10 Facebook account TRORICE CRAWFORD.

11         25.     The investigation also revealed that between 2015 up to the present, BOLING  
12 and CRAWFORD communicated extensively over Facebook Messenger and other electronic  
13 communications (e.g., email) about targeting military-affiliated individuals, identity theft, the  
14 unauthorized transfer of money to money mule accounts, and the remittance of these stolen  
15 funds to the Philippines via Western Union and MoneyGram. For example:

16           a. Records received from a search warrant on CRAWFORD's email  
17 account (cashmirepurple@gmail.com) include e-mail traffic from 2015 to present between  
18 CRAWFORD and BOLING (ctm1172@gmail.com) concerning stolen PII, the identity theft  
19 scheme and remittance of stolen funds to the Philippines. Included in two such  
20 communications between CRAWFORD to BOLING on or about September 22, 2017 and  
21 June 20, 2018 are photos of MoneyGram receipts for transfers to the Philippines that show  
22 the sender as "Trorice Crawford," located in San Diego, with a telephone number of 619-372-  
23 5591 (CRAWFORD's phone).



1           b. On December 12 and 13, 2018, the following Facebook Messenger  
2 exchange occurred between BOLING (LIESURE SUIT LARRY) and CRAWFORD  
3 (SPRINGVALLEY SAYDAT) concerning identity theft and the unauthorized transfer of  
4 money from a victim's bank account:

5           LIESURE SUIT LARRY: "Usaa not ready yet?"

6           SPRINGVALLEY SAYDAT: "They haven't sent me all the information"

7           LIESURE SUIT LARRY: "Fsho"

8           SPRINGVALLEY SAYDAT: "Wells Fargo ---swift code\_wFBIus6s---  
9 U.S.routing #121042882\_\_#121000248..  
10 Account Type checking \_\_\_\_adress o. Account 3275 30th st San  
11 Diego CA 92104-3607\_\_\_\_\_user name Tanisha43wff\_\_social  
12 2602 D.o.b.3-30-76 email address Tamishaw34@gmail.com"

13           SPRINGVALLEY SAYDAT: "This account ready"

14           LIESURE SUIT LARRY: "Name and account number ? . . .  
15 And card pin"

16           SPRINGVALLEY SAYDAT: "Tamisha Williams 9692"

17           LIESURE SUIT LARRY: "There's no account number there bro"

18           SPRINGVALLEY SAYDAT: "Wait on now see I told this nigga the bitch is  
19 slow"

20           SPRINGVALLEY SAYDAT: "5398322908"

21           LIESURE SUIT LARRY: "Yoyoyoyoyo"

22           LIESURE SUIT LARRY: "It's time bro! I'm up on a GOOD ass wire bro!"

23           SPRINGVALLEY SAYDAT: "Yoo I'm up now"

24           SPRINGVALLEY SAYDAT: "Let see what's up with the account"

...

SPRINGVALLEY SAYDAT: "On the account now"

1 LIESURE SUIT LARRY: "It's cutoff time in an hour an 30 mins bro... no bs,  
2 we needs this faster than fast"

3 LIESURE SUIT LARRY: "I mean... I got all the info I jus need u to tell me  
4 it's good and how much u feel me?"

5 SPRINGVALLEY SAYDAT: "But I needs that hella fast before 1 hour or we  
6 ain't gettin paid today ...and I'm broke so if I don't get paid ima die lolo"

7 c. As recently as February 9, 2019, the following Facebook Messenger  
8 exchange between CRAWFORD (SPRING VALLEYSAYDAT) and BOLING (LIESURE  
9 SUIT LARRY) occurred:

10 SPRINGVALLEY SAYDAT: "Send me the account information bro"

11 LIESURE SUIT LARRY: "Larry Pettingill in Idaho Falls, Idaho... bank is  
12 Mountain America Credit Union..."

13 LIESURE SUIT LARRY: "\$13,500USD"

14 SPRINGVALLEY SAYDAT: "My boy get off of work at 2"

15 SPRINGVALLEY SAYDAT: "My boy on his way to get him now"

16 LIESURE SUIT LARRY: "Fsho"

17 SPRINGVALLEY SAYDAT: "Just got him we on are way to the bank 🏠  
18 now"

19 LIESURE SUIT LARRY: "Ok bro"

20 LIESURE SUIT LARRY: "Godspeed!"

21 SPRINGVALLEY SAYDAT: "Yoo he went in they said it's hold on the  
22 money that just came in"

23 SPRINGVALLEY SAYDAT: "Still pending"

24 SPRINGVALLEY SAYDAT: "Think we have to wait tell tomorrow broide"

LIESURE SUIT LARRY: "They hatin bro!"

LIESURE SUIT LARRY: "You gotta go to another branch... or use the card  
at the atm bro..."

1 LIESURE SUIT LARRY: "Ain't no hold bro, you already know! It's a wire  
transfer just like all the rest, feel me?"

2 SPRINGVALLEY SAYDAT: "Yea"

3 SPRINGVALLEY SAYDAT: "I'm on it broide"

4 SPRINGVALLEY SAYDAT: "Now they tell him it's not there"

5 SPRINGVALLEY SAYDAT: "Bro check the account broide"

6 SPRINGVALLEY SAYDAT: "Send me pic"

7 SPRINGVALLEY SAYDAT: "Of everything"

8 LIESURE SUIT LARRY: "I'm checking hold up"

9 LIESURE SUIT LARRY: "It's there bro... available... \$13,500 or some  
10 shit..."


11 SPRINGVALLEY SAYDAT: "Yup"

12 ...

13 LIESURE SUIT LARRY: "Bro... the phone banking lady said it's available  
and you can get it at the branch"

14 ...

15 LIESURE SUIT LARRY: "Try the atm again bro... she said the card works  
and it's active"

16 SPRINGVALLEY SAYDAT: "Ok bro we going get def bank  and see  
what's up"

17 LIESURE SUIT LARRY: "Use the atm bro... if the atm works and this lady  
18 is right. Then they cant say it's hold feel me?"

19 SPRINGVALLEY SAYDAT: "Right p"

20 LIESURE SUIT LARRY: "When you go to another branch, tell them you  
21 already talked to phone banking and they said it's available and you can  
22 withdraw the money in the branch anytime..."

23 LIESURE SUIT LARRY: "What's good bro?"

24 LIESURE SUIT LARRY: "Did the atm work?"

...

LIESURE SUIT LARRY: "Bro! I see got \$8000!!"

LIESURE SUIT LARRY: "Ok yup"

LIESURE SUIT LARRY: "In the ATM? That's gangsta! Lol"

LIESURE SUIT LARRY: "Now get the last \$5500 in the branch?"

26. Further, I believe that this identity theft ring has been involved in more recent identity theft and money laundering activities. The investigation has revealed that as recently as July 29, 2019, the PII of a military-affiliated individual was exploited in a manner consistent with the scheme employed by BOLING's identity theft ring,<sup>7</sup> which resulted in an unauthorized wire transfer of approximately \$12,500 from the victim's Pentagon Federal Credit Union (PENFED) account into a Wells Fargo bank account owned by a money mule.

#### **PROBABLE CAUSE AS TO SUBJECT PREMISES**

27. I have reviewed the records provided by Cox Communication pursuant to a subpoena issued on July 17, 2019 and the records provided by Metro PCS / T-Mobile pursuant to a subpoena issued on June 19, 2019. The Cox Communications records indicated that as of June 17, 2019, the following address and home number are linked to the subscriber information for Trorice H. Crawford: 4078 34<sup>th</sup> Street, San Diego, CA and (619) 372-5591. The Metro PCS/T-Mobile records also confirm that the subscriber associated with (619) 372-5591 is Trorice Crawford.

---

<sup>7</sup> The individual that contacted the victim's bank spoofed the caller ID to show the calls originating from a phone number on file for the victim. PENFED recorded the call. Upon information and belief, the individual that contacted the bank was BOLING. BOLING, who as of August 6, 2019 is in custody, also admitted to being the voice behind various calls, similar to the aforementioned call, to other U.S. financial institutions.



28. Records from Cox Communications produced pursuant to a subpoena further revealed that between on or about April 2, 2019 and June 17, 2019, CRAWFORD's "SPRINGVALLEY SAYDAT" Facebook account was accessed from the following IP addresses:

2600:8801:9500:0lce:7950:8clb:7d7c:6e08,  
 2600:8801:9500:0lce:6d4a:ed07:857c:eca7, 2600:8801:9500:0lce:6579:3c93:7204:8040,  
 2600:8801:9500:0lce:044d:a2a2:9ad0:1370, 2600:8801:9500:0lce:d4d8:02a2:caf4:bef7,  
 2600:8801:9500:1297:6d0e:6dld:b786:dcdc, 2600:8801:9500:1297:c144:53cc:c82d:36cl,  
 2600:8801:9500:1297:148d:bcb3:c213:648c, 2600:8801:9500:1297:680d:85fa:110d:b694,  
 2600:8801:9500:1297:9193:81be:638c:2b69, 2600:8801:9500:1297:e9d7:00f4:8e41:ecf9,  
 2600:8801:9500:1297:f50f:e090:cbdf:6396, 2600:8801:9500:1297:7d71:60a7:f2c6:3e4d,  
 2600:8801:9500:1297:fc87:6bb8:b591:c8f4, 2600:8801:9500:0e68:8d93:9980:b705:55da,  
 2600:8801:9500:0e68:0lce:bb01:d26a:aabb and 2600:8801:9500:0e68:4d48:a852:dd30:29c3.

These IP addresses resolve to the SUBJECT PREMISES, *i.e.*, 4078 34<sup>th</sup> Street, San Diego, CA.

29. On July 16, 2019, agents observed CRAWFORD exiting and re-entering the SUBJECT PREMISES. CRAWFORD appeared to be removing trash from the SUBJECT PREMISES and discarding it in the trash bins located in the residence driveway. On July 31, 2019, agents took photographs of the SUBJECT PREMISES, which are included with Attachment A. On August 9, 2019, agents again observed CRAWFORD exiting the SUBJECT PREMISES though the front door.

30. Because the Facebook account CRAWFORD used to communicate with BOLING was accessed from IP addresses that resolved to 4078 34<sup>th</sup> Street, San Diego, CA, and because the primary means of communication amongst the co-conspirators has been Facebook Messenger and other electronic means (e.g. e-mail, text messaging), I believe that

1 evidence, fruits, or contraband may be found on computers or storage media located at the  
2 SUBJECT PREMISES. I also believe that the computers and/or storage mediums located on  
3 the SUBJECT PREMISES may be seized as contraband or instrumentalities.

4 **PROBABLE CAUSE AS TO DIGITAL DEVICES**

5 31. As described above and in Attachment B, this application seeks permission to  
6 search for records that might be found on the SUBJECT PREMISES, in whatever form they  
7 are found, including electronic storage media. Thus, the warrant applied for would authorize  
8 the seizure of electronic storage media or, potentially, the copying of electronically stored  
9 information, all under Rule 41(e) (2) (B).

10 32. I submit that if a computer or storage medium is found on the SUBJECT  
11 PREMISES, there is probable cause to believe the storage medium will contain evidence of  
12 the SUBJECT OFFENSES, for at least the following reasons.

13 a. Based on my knowledge, training, and experience, I know that computer  
14 files or remnants of such files can be recovered months or even years after they have been  
15 downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files  
16 downloaded to a storage medium can be stored for years at little or no cost. Even when files  
17 have been deleted, they can be recovered months or years later using forensic tools. This is so  
18 because when a person “deletes” a file on a computer, the data contained in the file does not  
19 actually disappear; rather, that data remains on the storage medium until it is overwritten by  
20 new data.

21 b. Therefore, deleted files, or remnants of deleted files, may reside in free  
22 space or slack space—that is, in space on the storage medium that is not currently being used  
23 by an active file—for long periods of time before they are overwritten. In addition, a  
24

1 computer's operating system may also keep a record of deleted data in a "swap" or "recovery"  
2 file.

3 c. Wholly apart from user-generated files, computer storage media—in  
4 particular, computers' internal hard drives—contain electronic evidence of how a computer  
5 has been used, what it has been used for, and who has used it. To give a few examples, this  
6 forensic evidence can take the form of operating system configurations, artifacts from  
7 operating system or application operation, file system data structures, and virtual memory  
8 "swap" or paging files. Computer users typically do not erase or delete this evidence, because  
9 special software is typically required for that task. However, it is technically possible to delete  
10 this information.

11 d. Similarly, files that have been viewed via the Internet are sometimes  
12 automatically downloaded into a temporary Internet directory or "cache."

13 33. Forensic evidence. As further described in Attachment B, of this application  
14 seeks permission to locate not only computer files that might serve as direct evidence of the  
15 crimes described on the warrant, but also for forensic electronic evidence that establishes how  
16 computers were used, the purpose of their use, who used them, and when. There is probable  
17 cause to believe that this forensic electronic evidence will be on any storage medium in the  
18 SUBJECT PREMISES because:

19 a. Data on the storage medium can provide evidence of a file that was once  
20 on the storage medium but has since been deleted or edited, or of a deleted portion of a file  
21 (such as a paragraph that has been deleted from a word processing file). Virtual memory  
22 paging systems can leave traces of information on the storage medium that show what tasks  
23 and processes were recently active. Web browsers, e-mail programs, and chat programs store  
24 configuration information on the storage medium that can reveal information such as online

1 nicknames and passwords. Operating systems can record additional information, such as the  
2 attachment of peripherals, the attachment of USB flash storage devices or other external  
3 storage media, and the times the computer was in use. Computer file systems can record  
4 information about the dates files were created and the sequence in which they were created,  
5 although this information can later be falsified.

6           b. As explained herein, information stored within a computer and other  
7 electronic storage media may provide crucial evidence of the “who, what, why, when, where,  
8 and how” of the criminal conduct under investigation, thus enabling the United States to  
9 establish and prove each element or, alternatively, to exclude the innocent from further  
10 suspicion. In my training and experience, information stored within a computer or storage  
11 media (e.g., registry information, communications, images and movies, transactional  
12 information, records of session times and durations, internet history, and anti-virus, spyware,  
13 and malware detection programs) can indicate who has used or controlled the computer or  
14 storage media. This “user attribution” evidence is analogous to the search for “indicia of  
15 occupancy” while executing a search warrant at a residence. The existence or absence of anti-  
16 virus, spyware, and malware detection programs may indicate whether the computer was  
17 remotely accessed, thus inculcating or exculpating the computer owner. Further, computer  
18 and storage media activity can indicate how and when the computer or storage media was  
19 accessed or used. For example, as described herein, computers typically contain information  
20 that log: computer user account session times and durations, computer activity associated  
21 with user accounts, electronic storage media that connected with the computer, and the IP  
22 addresses through which the computer accessed networks and the internet. Such information  
23 allows investigators to understand the chronological context of computer or electronic storage  
24 media access, use, and events relating to the crime under investigation. Additionally, some



1 information stored within a computer or electronic storage media may provide crucial  
2 evidence relating to the physical location of other evidence and the suspect. For example,  
3 images stored on a computer may both show a particular location and have geolocation  
4 information incorporated into its file data. Such file data typically also contains information  
5 indicating when the file or image was created. The existence of such image files, along with  
6 external device connection logs, may also indicate the presence of additional electronic  
7 storage media (e.g., a digital camera or cellular phone with an incorporated camera). The  
8 geographic and timeline information described herein may either inculcate or exculpate the  
9 computer user. Last, information stored within a computer may provide relevant insight into  
10 the computer user's state of mind as it relates to the offense under investigation. For example,  
11 information within the computer may indicate the owner's motive and intent to commit a  
12 crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g.,  
13 running a "wiping" program to destroy evidence on the computer or password  
14 protecting/encrypting such evidence in an effort to conceal it from law enforcement).

15 c. A person with appropriate familiarity with how a computer works can,  
16 after examining this forensic evidence in its proper context, draw conclusions about how  
17 computers were used, the purpose of their use, who used them, and when.

18 d. The process of identifying the exact files, blocks, registry entries, logs, or  
19 other forms of forensic evidence on a storage medium that are necessary to draw an accurate  
20 conclusion is a dynamic process. While it is possible to specify in advance the records to be  
21 sought, computer evidence is not always data that can be merely reviewed by a review team  
22 and passed along to investigators. Whether data stored on a computer is evidence may depend  
23 on other information stored on the computer and the application of knowledge about how a  
24

1 computer behaves. Therefore, contextual information necessary to understand other evidence  
2 also falls within the scope of the warrant.

3 e. Further, in finding evidence of how a computer was used, the purpose of  
4 its use, who used it, and when, sometimes it is necessary to establish that a particular thing is  
5 not present on a storage medium. For example, the presence or absence of counter-forensic  
6 programs or anti-virus programs (and associated data) may be relevant to establishing the  
7 user's intent.

8 f. I know that when an individual uses a computer to obtain unauthorized  
9 access to a victim's PII, bank account, veterans benefits accounts, and/or government-  
10 benefits accounts, or unauthorized access to government-benefits programs and websites (e.g.  
11 Defense Self-Service Logon ("DS Logon") or eBenefits) over the Internet, the individual's  
12 computer will generally serve both as an instrumentality for committing the crime, and also  
13 as a storage medium for evidence of the crime. The computer is an instrumentality of the  
14 crime because it is used as a means of committing the criminal offense. The computer is also  
15 likely to be a storage medium for evidence of crime. From my training and experience, I  
16 believe that a computer used to commit a crime of this type may contain: data that is evidence  
17 of how the computer was used; data that was sent or received; notes as to how the criminal  
18 conduct was achieved; records of Internet discussions about the crime; and other records that  
19 indicate the nature of the offense.

20 34. Because several people may share the SUBJECT PREMISES as a residence, it  
21 is possible that the SUBJECT PREMISES will contain storage media that are predominantly  
22 used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless  
23 determined that that it is possible that the things described in this warrant could be found on  
24

1 any of those computers or storage media, the warrant applied for would permit the seizure  
2 and review of those items as well.

3 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION**  
4 **AS TO ANY COMPUTER AND OTHER ELECTRONIC STORAGE DEVICES**

5 35. With the approval of the Court in signing this warrant, agents executing this  
6 search warrant will employ the following procedures regarding computers and other  
7 electronic storage devices, including electronic storage media that may contain data subject  
8 to seizure pursuant to this warrant.

9 **Seizure and Retention of Instrumentalities**

10 36. Based upon the foregoing, there is probable cause to believe that any computers  
11 and other electronic storage devices encountered during this search are instrumentalities of  
12 the enumerated offenses because there is probable cause to believe that they may contain  
13 contraband and fruits of crime as provided under Federal Rule of Criminal Procedure 41(c)(2)  
14 or were used in committing crime as provided under Federal Rule of Criminal Procedure  
15 41(c)(3). Consequently, the computers and any other electronic storage devices are subject to  
16 seizure, retention, and possible forfeiture and destruction. Computers, other electronic storage  
17 devices, and media confirmed onsite to contain contraband constitute fruits of crime or to  
18 have been used to commit a crime will not be returned but will be imaged offsite and analyzed.  
19 The onsite confirmation may be provided by an owner or user of the computer or storage  
20 device or, if feasible, may be obtained by conducting a limited onsite forensic examination to  
21 determine if the subject media contains any contraband or otherwise is an instrumentality.  
22 Computers and other electronic storage devices and media that are not confirmed onsite as  
23 instrumentalities will be taken offsite for imaging and preliminary analysis.  
24





1 drive, the longer it takes. As additional devices and hard drives are added, the length of time  
2 that the agents must remain onsite can become dangerous and impractical.

3 39. If it is not feasible to image the data on-site, computers and other electronic  
4 storage devices, including any necessary peripheral devices, will be transported offsite for  
5 imaging. After verified images have been obtained, the owner of the devices will be notified  
6 and the original devices returned within forty-five (45) days of seizure absent further  
7 application to this court.

#### 8 Identification and Extraction of Relevant Data

9 40. After obtaining a forensic image, the data will be analyzed to identify and  
10 extract data subject to seizure pursuant to this warrant. Analysis of the data following the  
11 creation of the forensic image can be a highly technical process requiring specific expertise,  
12 equipment and software. There are thousands of different hardware items and software  
13 programs, and different versions of the same programs, that can be commercially purchased,  
14 installed, and custom-configured on a user's computer system. Computers are easily  
15 customized by their users. Even apparently identical computers in an office or home  
16 environment can be different with respect to configuration, including permissions and access  
17 rights, passwords, data storage, and security. It is not unusual for a computer forensic  
18 examiner to have to obtain specialized hardware or software, and train with it, in order to  
19 view and analyze imaged data.

20 41. Analyzing the contents of a computer or other electronic storage device, even  
21 without significant technical challenges, can be very challenging. Searching by keywords, for  
22 example, often yields many thousands of hits, each of which must be reviewed in its context  
23 by the examiner to determine whether the data is within the scope of the warrant. Merely  
24 finding a relevant hit does not end the review process for several reasons. The computer may

1 have stored metadata and other information about a relevant electronic record – e.g., who  
2 created it, when and how it was created or downloaded or copied, when it was last accessed,  
3 when it was last modified, when it was last printed, and when it was deleted. Keyword  
4 searches may also fail to discover relevant electronic records, depending on how the records  
5 were created, stored, or used. For example, keywords search text, but many common  
6 electronic mail, database, and spreadsheet applications do not store data as searchable text.  
7 Instead, the data is saved in a proprietary non-text format. Documents printed by the  
8 computer, even if the document was never saved to the hard drive, are recoverable by forensic  
9 programs because the printed document is stored as a graphic image. Graphic images, unlike  
10 text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as  
11 graphic images and not as text. In addition, a particular relevant piece of data does not exist  
12 in a vacuum. To determine who created, modified, copied, downloaded, transferred,  
13 communicated about, deleted, or printed the data requires a search of other events that  
14 occurred on the computer in the time periods surrounding activity regarding the relevant data.  
15 Information about which user had logged in, whether users share passwords, whether the  
16 computer was connected to other computers or networks, and whether the user accessed or  
17 used other programs or services in the time period surrounding events with the relevant data  
18 can help determine who was sitting at the keyboard.

19 42. It is often difficult or impossible to determine the identity of the person using  
20 the computer when incriminating data has been created, modified, accessed, deleted, printed,  
21 copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers  
22 generate substantial information about data and about users that generally is not visible to  
23 users. Computer-generated data, including registry information, computer logs, user profiles  
24 and passwords, web-browsing history, cookies and application and operating system

1 metadata, often provides evidence of who was using the computer at a relevant time. In  
2 addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars  
3 and address books stored on the computer may identify the user at a particular, relevant time.  
4 The manner in which the user has structured and named files, run or accessed particular  
5 applications, and created or accessed other, non-incriminating files or documents, may serve  
6 to identify a particular user. For example, if an incriminating document is found on the  
7 computer but attribution is an issue, other documents or files created around that same time  
8 may provide circumstantial evidence of the identity of the user that created the incriminating  
9 document.

10 43. Analyzing data has become increasingly time-consuming as the volume of data  
11 stored on a typical computer system and available storage devices has become mind-boggling.  
12 For example, a single megabyte of storage space is roughly equivalent of 500 double-spaced  
13 pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent  
14 of 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal  
15 computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may  
16 be stored in a variety of formats or encrypted (several new commercially available operating  
17 systems provide for automatic encryption of data upon shutdown of the computer). The sheer  
18 volume of data also has extended the time that it takes to analyze data. Running keyword  
19 searches takes longer and results in more hits that must be individually examined for  
20 relevance. And, once reviewed, relevant data leads to new keywords and new avenues for  
21 identifying data subject to seizure pursuant to the warrant.

22 44. Based on the foregoing, identifying and extracting data subject to seizure  
23 pursuant to this warrant may require a range of data analysis techniques, including hashing  
24 tools to identify data subject to seizure pursuant to this warrant, and to exclude certain data

1 from analysis, such as known operating system and application files. The identification and  
2 extraction process, accordingly, may take weeks or months. The personnel conducting the  
3 identification and extraction of data will complete the analysis within one-hundred twenty  
4 (120) days of this warrant, absent further application to this court.

5 45. All forensic analysis of the imaged data will employ search protocols directed  
6 exclusively to the identification and extraction of data within the scope of this warrant.

7 Genuine Risks of Destruction

8 46. Based upon my experience and training, and the experience and training of  
9 other agents with whom I have communicated, electronically stored data can be permanently  
10 deleted or modified by users possessing basic computer skills. In this case, only if the subject  
11 receives advance warning of the execution of this warrant, will there be a genuine risk of  
12 destruction of evidence.

13 Prior Attempts to Obtain Data

14 47. The United States has not attempted to obtain this data by other means.

15 **PROCEDURES FOR ELECTRONICALLY STORED INFORMATION ON**  
16 **CELLULAR TELEPHONES**

17 48. It is not possible to determine, merely by knowing the cellular telephone's  
18 make, model, and serial number, the nature and types of services to which the device is  
19 subscribed and the nature of the data stored on the device. Cellular devices today can be  
20 simple cellular telephones and text message devices, can include cameras, can serve as  
21 personal digital assistants and have functions such as calendars and full address books and  
22 can be mini-computers allowing for electronic mail services, web services and rudimentary  
23 word processing. An increasing number of cellular service providers now allow for their  
24 subscribers to access their device over the internet and remotely destroy all of the data



1 contained on the device. For that reason, the device may only be powered in a secure  
2 environment or, if possible, started in "flight mode" which disables access to the network.  
3 Unlike typical computers, many cellular telephones do not have hard drives or hard drive  
4 equivalents and store information in volatile memory within the device or in memory cards  
5 inserted into the device. Current technology provides some solutions for acquiring some of  
6 the data stored in some cellular telephone models using forensic hardware and software. Even  
7 if some of the stored information on the device may be acquired forensically, not all of the  
8 data subject to seizure may be so acquired. For devices that are not subject to forensic data  
9 acquisition or that have potentially relevant data stored that is not subject to such acquisition,  
10 the examiner must inspect the device manually and record the process and the results using  
11 digital photography. This process is time and labor intensive and may take weeks or longer.

12 49. Following the issuance of this warrant, I will collect CRAWFORD's cellular  
13 telephone and subject it to analysis. All forensic analysis of the data contained within the  
14 telephone and its memory cards will employ search protocols directed exclusively to the  
15 identification and extraction of data within the scope of this warrant.

16 50. Based on the foregoing, identifying and extracting data subject to seizure  
17 pursuant to this warrant may require a range of data analysis techniques, including manual  
18 review, and, consequently, may take weeks or months. The personnel conducting the  
19 identification and extraction of data will complete the analysis within ninety (90) days of the  
20 date the warrant is signed, absent further application to this court.

#### 21 **PROTOCOL FOR EVIDENCE OF OTHER CRIMES**

22 51. The search methodology for this matter will be formulated to provide for the  
23 search and seizure of the items authorized to be seized by the warrant. In the course of that  
24 examination, the examiner may discover evidence that is not authorized for seizure, but

1 which nonetheless constitutes evidence of other crimes (“inadvertent discovery”). In the event  
2 of inadvertent discovery of evidence of a crime not authorized for seizure by the warrant, the  
3 following procedures will apply.

4 52. The government will only seize or investigate evidence of other crimes that is  
5 inadvertently discovered during the course of a search authorized by this federal warrant after  
6 additional appropriate legal process.

7 53. The examiner will continue with the search for the items to be seized, as  
8 authorized by the warrant, and will segregate the inadvertently discovered evidence from the  
9 authorized search. The examiner will not, without further authorization of the court, amend  
10 or expand the search criteria to include the inadvertently discovered information.

11 54. The examiner will not separately provide the inadvertently discovered evidence  
12 to the agents and prosecutors involved in the investigation.

13 **SEALING REQUEST**

14 55. It is respectfully requested that this Court issue an order sealing, until further  
15 order of the Court, all papers submitted in support of this application, including the  
16 Application, Affidavit, and search warrant. I believe that sealing this document is necessary  
17 because the items and information to be seized are relevant to an ongoing investigation of an  
18 extensive identify theft ring and, at this time, not all of the targets of this investigation will be  
19 searched. Based upon my training and experience, I have learned that online criminals  
20 actively search for criminal affidavits and search warrants via the Internet, and disseminate  
21 them to other online criminals as they deem appropriate, i.e., post them publicly online  
22 through the carding forums. Premature disclosure of the contents of this Affidavit and related  
23 documents may have a significant and negative impact on the continuing investigation and  
24 may severely jeopardize its effectiveness.

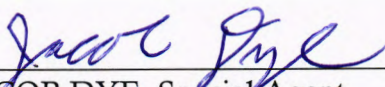
CONCLUSION

56. Based on the above facts set forth, I believe there is probable cause that the SUBJECT PREMISES contain evidence, fruits, or instrumentalities of the SUBJECT OFFENSES.

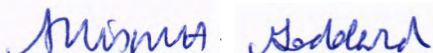
57. Accordingly, I respectfully request that the Court issue search warrants authorizing any law enforcement law officers to search the SUBJECT PREMISES (described in Attachment A), and to seize and to search for the items listed in Attachment B, all of which constitute evidence, fruits, or instrumentalities of the SUBJECT OFFENSES.

I swear, under penalty of perjury, that the foregoing is true and correct to the best of my knowledge and belief.

Respectfully Submitted,

  
JACOB DYE, Special Agent  
Defense Criminal Investigative Services

SUBSCRIBED AND SWORN  
before me this 15<sup>th</sup> day of August, 2019.

  
HONORABLE ALLISON GODDARD  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**PREMISES TO BE SEARCHED**

The property to be searched is 4078 34<sup>th</sup> Street, San Diego, CA 92104, further described as the left-side of a one-level tan in color residential duplex. Photographs of the SUBJECT PREMISES are included below.





**ATTACHMENT B**

**ITEMS TO BE SEARCHED FOR AND SEIZED**

1. The evidence to be searched for and seized concerns evidence, contraband, fruits, or instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1349 (conspiracy to commit wire fraud), 1956 (conspiracy to commit money laundering) and 1028A (aggravated identity theft), committed between July 1, 2014, and August 6, 2019 is described as follows:

a. Communications, papers, records and information relating to a conspiracy to defraud victims with a military association (those on active duty, reservists, retired service members, military spouses, and military dependents) (hereafter “military-affiliated individuals”);

b. Communications, records and information relating to access of military-affiliated individuals’ computers, bank accounts, veterans benefits accounts and other government-benefits accounts, and/or government-benefits program websites (e.g., DS Logon or eBenefits);

c. Records and information relating to financial transactions using funds obtained from victim bank accounts;

d. Records and information relating to financial transactions concerning the remittance of stolen funds via money transfers (e.g. Western Union, MoneyGram, etc.) to foreign entities;

e. Records and information relating to the following e-mail accounts, their ownership and control, and use of the email accounts to further illicit activities: brown.fredrick@gmail.com (associated with BROWN); fastcask2k10@aol.com and

1 cashmirepurple@gmail.com (associated with CRAWFORD); and ctm1172@gmail.com,  
2 bolingjunior@gmail.com, and wayneboling0600@gmail.com (associated with BOLING) ;

3 f. Communications with the e-mail accounts listed above in paragraph  
4 1.e. or other e-mail accounts linked to other co-conspirators concerning the SUBJECT  
5 OFFENSES;

6 g. Records and information exchanged via Facebook Messenger or  
7 stored in Dropbox accounts (or other cloud storage accounts) of the co-conspirators  
8 concerning stolen PII and other aspect of the conspiracy to defraud military-affiliated  
9 individuals;

10 h. Records and information relating to the identity or location of the  
11 suspects and other accomplices/co-conspirators;

12 i. Records and information relating to communications with Internet  
13 Protocol (IP) address 120.29.124.34 or any other IP address who initial 5 digit numerical  
14 label resolves to 120.29.

15 j. Records and information relating to the un authorized access and/or  
16 theft of electronic health records of military-affiliated individuals and/or the Armed Forces  
17 Health Longitudinal Technology Application (AHLTA);

18 k. Records and information relating to malicious software.

19 l. Routers, modes, and network equipment used to connect digital  
20 devices to the Internet;

21 m. Any digital device used to facilitate the above-listed violations and  
22 forensic copies thereof;

23 n. Any digital device capable of storing or containing the documents,  
24 records, and communications mentioned in items a through j above;

1           o.       With respect to any seized digital device, the following information is  
2 also to be seized:

3                   i.       evidence of who used, owned, or controlled the device at the  
4 time the things described in this warrant were created, edited, or deleted, such as logs,  
5 registry entries, configuration files, saved usernames and passwords, documents, browsing  
6 history, user profiles, e-mail, e-mail contacts, chat and instant messaging logs, photographs,  
7 and correspondence;

8                   ii.      evidence of the presence or absence of software that would  
9 allow others to control the device, such as viruses, Trojan horses, and other forms of  
10 malicious software, as well as evidence of the presence or absence of security software  
11 designed to detect malicious software;

12                  iii.     evidence of the attachment to the device of other storage  
13 devices or similar containers for electronic evidence;

14                  iv.     evidence of counter-forensic programs (and associated data)  
15 that are designed to eliminate data from the device;

16                  v.      evidence indicating how and when the device was accessed or  
17 used to determine the chronological context of device access, use, and events relating to  
18 crime under investigation and to the device user;

19                  vi.     evidence indicating the device user's state of mind as it relates  
20 to the crime under investigation;

21                  vii.    evidence of the times the device was used;

22                  viii.   passwords, encryption keys, biometric keys, and other access  
23 devices that may be necessary to access the device;

ix. applications, utility programs, compilers, interpreters, or other software, as well as documentation and manuals, that may be necessary to access the device or to conduct a forensic examination of it;

x. records or information about Internet Protocol addresses used by the device;

xi. records of or information about the device's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

xii. contextual information necessary to understand the evidence described in this attachment.

2. The seizure and search of digital devices shall follow the procedures outlined in the supporting affidavit. Deleted data, remnant data, slack space, and temporary and permanent files on the digital devices may be searched for the evidence above.



UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
SAN ANTONIO DIVISION

FILED

JUL 23 2019

CLERK, U.S. DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
BY 6 DEPUTY

UNITED STATES OF AMERICA

§ CRIMINAL NO.

v.

§  
§ SEALED  
§ INDICTMENT

**SA 19 CR 0524 OG**

ROBERT WAYNE BOLING, JR. (1),  
FREDRICK BROWN (2),  
TRORICE CRAWFORD (3),  
ALLAN ALBERT KERR (4), and  
JONGMIN SEOK (5)

§ COUNT 1: 18 U.S.C. § 1349, Conspiracy  
§ to Commit Wire Fraud  
§ COUNTS 2-7: 18 U.S.C. § 1343 and 2,  
§ Wire Fraud  
§ COUNT 8: 18 U.S.C. § 1956, Conspiracy  
§ to Commit Money Laundering  
§ COUNTS 9-14: 18 U.S.C. § 1028A,  
§ Aggravated Identity Theft

§  
§ NOTICE OF GOVERNMENT'S  
§ DEMAND FOR FORFEITURE  
§  
§

THE GRAND JURY CHARGES:

THE CONSPIRACY

At all times relevant herein:

OVERVIEW

1. Beginning in and around July 2014, and continuing through in or around July 2019, the Defendants, **ROBERT WAYNE BOLING, JR. ("BOLING")**, **FREDRICK BROWN ("BROWN")**, **TRORICE CRAWFORD ("CRAWFORD")**, **ALLAN ALBERT KERR ("KERR")**, and **JONGMIN SEOK ("SEOK")**, together with others known and

unknown to the Grand Jury, perpetrated a scheme to exploit stolen personal identifying information (“PII”) belonging to members of the United States military, including service members (active duty, reserve component, and National Guard) and veterans, their dependents, and civilians employed by the Department of Defense (collectively, “military-affiliated individuals”). The Defendants used the stolen PII to target military-affiliated individuals in various ways, such as stealing from military-affiliated individuals’ personal bank accounts and stealing pension and disability benefits paid to military-affiliated individuals by the Veterans Administration (“veterans benefits”). The Defendants then made financial transactions involving numerous bank accounts and money remittances to conceal and dispose of stolen monies.

2. Over the course of the scheme, the Defendants stole and exploited the PII of thousands of military-affiliated individuals and caused millions of dollars of actual and attempted losses to military-affiliated individuals, the Veterans Administration, and banks and credit unions across the United States.

3. The Defendants generally played the following roles in the scheme:

- a. **BOLING** was the principal orchestrator of the scheme. **BOLING** received stolen PII, and coordinated with and directed other Defendants and others to exploit the stolen PII in order to compromise military-affiliated individuals’ bank accounts, steal military-affiliated individuals’ veterans benefits, and remit stolen funds to the Philippines. **BOLING**, an American citizen raised in South Korea as a United States military dependent, lived in Angeles City, Philippines.
- b. **BROWN** was the primary source of stolen PII. From December 2010 through September 2015, **BROWN** had worked as a civilian medical records technician at the 65<sup>th</sup> Medical Brigade, United States Army, at Yongsan Garrison, South Korea.

In that capacity, **BROWN** had access to a substantial volume of military-affiliated individuals' PII, which he copied and transmitted to **BOLING**.

- c. **CRAWFORD** acted as a recruiter and supervisor of individuals who provided their bank accounts to be used to receive stolen funds ("money mules").

**CRAWFORD**, an American citizen living in the vicinity of San Diego, California, coordinated with **BOLING** to transfer funds stolen from military-affiliated individuals to be deposited into money mules' accounts. **CRAWFORD** also assisted in remitting stolen funds from money mules' accounts to members of the conspiracy in the Philippines.

- d. **KERR** and **SEOK** assisted **BOLING** in using military-affiliated individuals' PII to obtain additional records of military-affiliated individuals to facilitate the scheme, such as credit reports and official military personnel files. Like **BOLING**, **KERR** (an Australian citizen) and **SEOK** (a South Korean citizen) lived in Angeles City, Philippines (collectively, the Philippines Defendants).

#### **OBJECT OF THE CONSPIRACY**

- 4. The object of the conspiracy was to enrich the Defendants by stealing money and property from military-affiliated individuals, government-benefit programs, and financial institutions by means of identity theft, fraud, and money laundering.

#### **MANNER AND MEANS OF THE CONSPIRACY**

- 5. The scheme and artifice to defraud was carried out in the manner and means described below.

### **Theft of Military-Affiliated Individuals' PII**

6. From in and around December 2010 through in and around September 2015, while employed as a medical records technician at Yongsan Garrison, **BROWN** worked with a database called the Armed Forces Health Longitudinal Technology Application (“AHLTA”), which is one of the United States military’s principal repositories for electronic health records of military-affiliated individuals. As a medical records technician, **BROWN** had access to substantial volumes of military-affiliated individuals’ PII. Specifically, beyond health-related data, AHLTA contained each military-affiliated individual’s name, social security number, Department of Defense ID number (a unique 10-digit number assigned to military-affiliated individuals), date of birth, gender, mailing address, and telephone number. AHLTA was designed in such a way that the user could view the PII for approximately ten different military-affiliated individuals simultaneously.

7. While employed at the 65<sup>th</sup> Medical Brigade, **BROWN** took digital photographs of thousands of military-affiliated individuals’ PII displayed in AHLTA in groups of ten. **BROWN** conveyed these photographs to **BOLING** through various communication channels. **BOLING** knew that **BROWN** was taking photographs of his AHLTA computer screen in order to obtain military-affiliated individuals’ PII, at one point asking **BROWN** whether or not **BROWN** had gotten “popped red handed snappin shots at the gig.”

### **Exploitation of Military-Affiliated Individuals' PII**

#### ***DS Logon***

8. One of the principal means by which the Defendants exploited the stolen PII to commit identity theft was the compromise of military-affiliated individuals’ Department of Defense Self-Service Logon (“DS Logon”) accounts. DS Logon was a system that allowed



military-affiliated individuals access to more than 70 nonpublic websites using a single username and password. DS Logon was maintained by the Defense Manpower Data Center, the Department of Defense component agency responsible for maintaining data on U.S. military personnel. With a DS Logon account, a military-affiliated individual could access websites containing extensive personal and financial data, including PII for all of a military-affiliated individual's dependents (spouse and children), tax information, and health records, among other information. The user of a DS Logon account could also alter the account and routing numbers for bank accounts into which salaries, benefits, disability payments, and pensions were paid by the Department of Defense or the Veterans Administration. Without a DS Logon account, access to these websites required authentication using a common access card ("CAC"), a physical plastic card with an electronic chip in it that must be inserted into a keyboard or other device specifically designed to read it, or an in-person visit to a Department of Defense personnel office.

9. Creation of a DS Logon account required a user to visit a website maintained by the Defense Manpower Data Center and to input certain elements of a military-affiliated individual's PII. The user was also required to answer security questions based on entries in the military-affiliated individual's credit report. Correct responses to the security questions enabled the user to create a DS Logon account. This identity verification within the DS Logon system without the use of a CAC or an in-person visit to a Department of Defense personnel office was called "remote proofing." The DS Logon system also permitted identity verification via remote proofing for existing DS Logon accounts. A user could reset the username and password associated with an existing account by answering security questions to establish new credentials. Once a new password was established and the user had gained access to the DS Logon account,

the user could change the contact information the system used to notify the user of subsequent changes to the account.

10. Over the course of the scheme, the Defendants used the photographs of the AHLTA screens taken by **BROWN**, containing PII of thousands of military-affiliated individuals in the manner described above, to create and compromise DS Logon accounts.

***eBenefits***

11. One of the partner sites that could be accessed using a DS Logon credential was “eBenefits,” a web portal hosted by the Veterans Administration within the Western District of Texas. The servers through which all online communication with eBenefits flowed, and the administrative staff that supported the website, were physically located within the Western District of Texas. The eBenefits web portal provided military-affiliated individuals the ability to manage their Veterans Administration and Department of Defense benefits, claims, and military documents online.

12. The Defendants accessed eBenefits in furtherance of two related types of fraud against military-affiliated individuals.

***a. Theft of Funds from Military-Affiliated Individuals’ Personal Bank Accounts:***

Once logged into a military-affiliated individual’s DS Logon account, the Defendants accessed eBenefits in that military-affiliated individual’s name to obtain the account and routing number of the bank account into which the military-affiliated individual received veterans benefits. The Defendants then used that account and routing number combination, along with other PII, to steal money from the military-affiliated individual’s personal bank account. In some

instances, the Defendants contacted banks and other financial institutions by telephone, chat, and e-mail, and posed as military-affiliated individuals.

**b. *Theft of Veterans Benefits:***

The Defendants also accessed eBenefits to substitute a bank account they controlled for the military-affiliated individual's own bank account, so that any veterans benefit would be paid directly to the Defendants.

***Military-Focused Financial Institutions***

13. The Defendants also used means other than eBenefits to steal from military-affiliated individuals, targeting personal bank accounts held through certain financial institutions with a significant military clientele. At least two such military-focused financial institutions, United States Automobile Association ("USAA") and Randolph-Brooks Federal Credit Union ("Randolph-Brooks FCU"), were based within the Western District of Texas, in the vicinity of San Antonio. By exploiting military-affiliated individuals' PII stolen by **BROWN**, and obtained through eBenefits and elsewhere, the Defendants caused millions of dollars in actual and attempted losses to military-affiliated individuals from those individuals' bank accounts held through military-focused financial institutions across the United States.

***International Money Remittances***

14. The Philippines Defendants, **BOLING**, **KERR**, and **SEOK**, worked with a network of "money mules" – co-conspirators who provided bank accounts into which stolen funds could be deposited. The money mules tended to operate from various locations within the United States, including San Antonio, within the Western District of Texas. **CRAWFORD** supervised several of these money mules, and, on several occasions, **CRAWFORD** accompanied the money mules to various bank branches in the vicinity of San Diego, California,

and directed the money mules to withdraw funds deposited into their bank accounts by the Philippines Defendants. **CRAWFORD** provided **BOLING** with the money mules' bank account information, and **BOLING** transferred funds stolen from military-affiliated individuals into the money mules' accounts. **CRAWFORD** then kept a percentage of the withdrawn funds and oversaw the transmittal of the remainder by means of international money services businesses to recipients in the Philippines, including the Philippines Defendants themselves as well as other parties whose names **BOLING** provided to **CRAWFORD**.

***Example Acts in Furtherance of the Scheme***

15. Over the course of the conspiracy, the Defendants exploited thousands of military-affiliated individuals' PII. The Defendants often targeted older military-affiliated individuals, who were less likely to use DS Logon and eBenefits, and disabled veterans, who were more likely to receive larger veterans benefits. The following examples of acts in furtherance of the scheme were typical of those engaged in by the Defendants.

***a. Colonel H.C., United States Air Force***

- i. At some point prior to May 2015, the exact date being unknown to the Grand Jury, **BROWN** provided **BOLING** with the PII of at least 50 military-affiliated individuals who all had the same last name, a relatively uncommon three-letter name beginning with the letter C.
- ii. On or about May 14, 2015, **BOLING** used the PII of Colonel ("Col.") H.C., one of those 50 individuals with the same three-letter last name, to effectuate a wire transfer in the amount of \$16,250 from Col. H.C.'s USAA bank account to a Wells Fargo bank account in the name of G.H., a money mule.



- iii. That same day, **BOLING** provided the following instructions to a member of the conspiracy:

From usaa bank of [H.C.] in...GA. Tell him take out 14 or 15 k...I just need 7000 even....

Tell him to have a good story... Just tell him to say its his uncle sending money for his family or some shit but not too much detail....

...In fact i have a perfect idea... Send me 3000 all at once asap and then send 2000 to Fredrick Brown in Western Union... Please confirm so i can tell Fred.

- iv. On or about May 18, 2015, after the funds had been transferred to the account of G.H., **BOLING** expressed concern to **BROWN** that G.H. was delayed in remitting the funds stolen from Col. H.C. **BOLING** then asked **BROWN** for additional information on G.H. (also a U.S. military dependent) and G.H.'s family, for the purpose of threatening G.H.'s family members if G.H. did not send the funds promptly. In response, **BROWN** then queried G.H.'s electronic health record in AHLTA, which included information on G.H.'s family. Shortly thereafter, G.H. then sent a portion of the money stolen from Col. H.C.'s account to the Philippines as directed by **BOLING**.

***b. Petty Officer First Class A.D., United States Navy***

- i. On or about October 19, 2016, a member of the conspiracy based in the Philippines conducted initial registration of the eBenefits account of Petty Officer First Class ("PO1") A.D., and thereby obtained the account and

routing information of the account held through Kitsap Federal Credit Union (“Kitsap FCU”) into which PO1 A.D.’s veterans benefit was paid.

- ii. On that date in October 2016, PO1 A.D. was 79 years old, and had never used DS Logon or eBenefits.
- iii. On or about October 24, 2016, **BOLING** contacted Kitsap FCU customer service, and impersonated PO1 A.D.
- iv. Over the course of the following two days, **BOLING** arranged two wire transfers out of the bank account of PO1 A.D. The first wire transfer, in the amount of \$18,500, was successfully deposited into the bank account of a member of the conspiracy. Following that transfer, PO1 A.D. contacted Kitsap FCU customer service, and advised that the wire had been unauthorized. **BOLING** then attempted a second wire transfer in the amount of \$27,000 from PO1 A.D.’s account, which was denied as unauthorized. Kitsap FCU then closed PO1 A.D.’s account, and assigned PO1 A.D. a new Kitsap FCU account number.
- v. On or about November 18, 2016, **SEOK** accessed the eBenefits account of PO1 A.D. **SEOK** took screen captures from within PO1 A.D.’s eBenefits account, capturing his PII, including PO1 A.D.’s Veterans Administration file number, and the account and routing number for PO1 A.D.’s new Kitsap FCU account after the unauthorized wires orchestrated by **BOLING** in October 2016.
- vi. On or about December 15, 2016, a member of the conspiracy accessed PO1 A.D.’s eBenefits account and substituted a Community Federal

Savings Bank account and routing number in place of the Kitsap FCU account details on file with the Veterans Administration.

- vii. On or about December 20, 2016, PO1 A.D.'s veterans benefit, in the amount of \$1,451.71, was paid to the Community Federal Savings Bank account, instead of PO1 A.D.'s own account.

*c. Major R.W., United States Army*

- i. On or about March 6, 2017, **BOLING** accessed the DS Logon account of Major ("Maj.") R.W., and e-mailed a screenshot to **SEOK** of Maj. R.W.'s profile screen from within DS Logon.
- ii. On that date in March 2017, Maj. R.W. was 76 years old. Maj. R.W. was a 100% service-connected disabled veteran, and had been a prisoner of war.
- iii. Approximately 20 minutes later, **SEOK** accessed Maj. R.W.'s eBenefits account. **SEOK** then e-mailed **BOLING** photographs of **SEOK**'s laptop screen showing the profile page for Maj. R.W.'s eBenefits account. The subject line of the e-mail from **SEOK** to **BOLING** read "Have Big money. may be.."
- iv. Approximately 10 minutes later, **SEOK** conveyed to **BOLING** certain details about Maj. R.W.'s veteran status, including Maj. R.W.'s disability benefit amount, the USAA bank account and routing numbers into which his disability benefit was being paid, and a screenshot from within eBenefits showing a list of Maj. R.W.'s service-connected disabilities.

- v. On or about April 16, 2017, a member of the conspiracy accessed Maj. R.W.'s eBenefits account and removed Maj. R.W.'s USAA bank account and routing information, substituting account and routing information of an American Express debit card account.
- vi. On or about April 19, 2017, Maj. R.W.'s monthly veterans benefit, in the amount of \$2,915.55, was paid into the American Express debit card account, instead of Maj. R.W.'s USAA bank account.

*d. Col. F.C., United States Air Force*

- i. On or about March 9, 2017, **SEOK** accessed both the DS Logon and eBenefits accounts of Col. F.C., who had the same three-letter last name as Col. H.C. (referenced above in paragraph 15a), and was also one of the approximately 50 individuals whose PII **BROWN** provided to **BOLING** no later than May 2015.
- ii. On that date in March 2017, Col. F.C. was 66 years old.
- iii. That same day, **SEOK** e-mailed to **BOLING** certain PII of Col. F.C. obtained from eBenefits, including the account and routing number of the Pentagon Federal Credit Union ("Pentagon FCU") account into which Col. F.C. received a veterans benefit. The subject line of the e-mail was "Pentagon."
- iv. Approximately one minute later, **BOLING** forwarded **SEOK**'s e-mail, including Col. F.C.'s PII and the subject line "Pentagon," to **KERR**.
- v. On or about March 28, 2017, a member of the conspiracy accessed Col. F.C.'s Pentagon FCU account online and took out a \$2,000 loan, which



was deposited to Col. F.C.'s checking account. At that time, Pentagon FCU identified the transaction as fraudulent and closed Col. F.C.'s account.

*e. Chief Petty Officer L.W., United States Navy*

- i. On or about October 10, 2017, **KERR** accessed the eBenefits account of Chief Petty Officer ("CPO") L.W.
- ii. That same day, **KERR** conveyed to **BOLING** certain PII of CPO L.W., including a credit report as well as the Navy Federal Credit Union ("Navy FCU") bank account and routing information of the account into which CPO L.W.'s monthly veterans benefit was paid and the contact telephone number on file with the Veterans Administration for CPO L.W.
- iii. On or about December 9, 2017, a member of the conspiracy called the customer service line of Navy FCU and impersonated CPO L.W., using call-spoofing technology to appear to be calling from the number on file with the Veterans Administration for CPO L.W. The caller was unable to answer all of the security questions posed by the customer service representative, and terminated the call without completing any transactions.

*f. Master Sergeant E.R., United States Air Force*

- i. On or about June 18, 2018, **BOLING** contacted **CRAWFORD** and arranged for a wire transfer from the Randolph-Brooks FCU account of Master Sergeant ("MSgt") E.R. **CRAWFORD** provided the name of D.B., a money mule, along with details of a Wells Fargo account in the

name of D.B., including the account and routing number, online banking username and password, and the contact information linked to D.B.'s account.

- ii. On that date in June 2018, E.R. was 73 years old, and a resident of New Braunfels, in the vicinity of San Antonio, Texas and within the Western District of Texas.
- iii. In response, the following day, **BOLING** wrote to **CRAWFORD** "The request sent...we on standby...\$9,600 from randolph brooks Credit union...Senders name I sent [E.R.] Jr. From Texas." **CRAWFORD** responded "...they keep say 24 hour wait the money there they said everything good but 24 hour hold." **BOLING** replied "Yeah it should be all good tomorrow... they used to do that shit to us always... just don't lose your boy by tomorrow."
- iv. That day, \$9,600 was wired from MSgt E.R.'s account to D.B.'s account.
- v. Between on or about June 19, 2018, and on or about June 27, 2018, **BOLING** arranged for a total of five wires, each between \$7,300 and \$9,600, to be sent from MSgt E.R.'s account to the account of D.B., for a total of \$41,500. D.B., under **CRAWFORD**'s supervision, withdrew funds from D.B.'s account shortly after each wire transfer and, by on or about June 27, 2018, D.B. had withdrawn the entire sum of \$41,500 from D.B.'s account.

**COUNT ONE**  
**Conspiracy to Commit Wire Fraud**  
**[18 U.S.C. § 1349]**

16. Count One incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

17. Beginning sometime in 2014, the exact date being unknown, and continuing until the date of this Indictment, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1),**  
**FREDRICK BROWN (2),**  
**TRORICE CRAWFORD (3),**  
**ALLAN ALBERT KERR (4), and**  
**JONGMIN SEOK (5)**

did knowingly and intentionally conspire and agree with others known and unknown to the Grand Jury to commit certain offenses against the United States, namely: Wire Fraud, in violation of 18 U.S.C. § 1343, that is, knowingly and with intent to defraud, having devised and having intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in this case, a fraudulent scheme to steal from military-affiliated individuals, for the purpose of executing the scheme and artifice, transmitted and caused to be transmitted by means of wire, radio and television communication in interstate commerce certain writings, signs, signals, pictures and sounds.

All in violation of Title 18, United States Code, Section 1349.

**COUNTS TWO THROUGH SEVEN****Wire Fraud****[18 U.S.C. §§ 1343 and 2]**

18. Counts Two through Seven incorporate by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

19. On or about the following dates, in the Western District of Texas and elsewhere, the Defendants, aiding and abetting each other, knowingly and with intent to defraud, having devised and having intended to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, in this case, a fraudulent scheme to steal from military-affiliated individuals, for the purpose of executing the scheme and artifice, transmitted and caused to be transmitted by means of wire, radio and television communication in interstate commerce certain writings, signs, signals, pictures and sounds to and from the Western District of Texas, as described below:

<b>COUNT</b>	<b>DATE</b>	<b>DEFENDANTS</b>	<b>DESCRIPTION</b>
2	May 14, 2015	<b>ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2)</b>	Wire transfer from the USAA bank account of victim H.C.
3	October 19, 2016	<b>ROBERT WAYNE BOLING, JR. (1), JONGMIN SEOK (5)</b>	Access to eBenefits account of victim A.D.
4	March 6, 2017	<b>ROBERT WAYNE BOLING, JR. (1), JONGMIN SEOK (5)</b>	Access to eBenefits account of victim R.W.
5	March 9, 2017	<b>ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2), ALLAN ALBERT KERR (4), JONGMIN SEOK (5)</b>	Access to eBenefits account of victim F.C.
6	October 10, 2017	<b>ROBERT WAYNE BOLING, JR. (1), ALLAN ALBERT KERR (4)</b>	Access to eBenefits account of victim L.W.



7	June 18, 2018	<b>ROBERT WAYNE BOLING, JR. (1), TRORICE CRAWFORD (3)</b>	Wire from the Randolph-Brooks FCU account of victim E.R.
---	---------------	---	---

All in violation of Title 18, United States Code, Sections 1343 and 2.

**COUNT EIGHT**  
**Conspiracy to Commit Money Laundering**  
**[18 U.S.C. § 1956(h)]**

20. Count Eight incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

21. Beginning sometime in 2014, the exact date being unknown, and continuing until the date of this Indictment, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1),  
FREDRICK BROWN (2),  
TRORICE CRAWFORD (3),  
ALLAN ALBERT KERR (4), and  
JONGMIN SEOK (5)**

did knowingly combine, conspire, and agree with other persons known and unknown to the Grand Jury to commit offenses against the United States in violation of Title 18, United States Code, Section 1956, namely: to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, Wire Fraud in violation of 18 U.S.C. § 1343, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

All in violation of Title 18, United States Code, Section 1956(h).

**COUNT NINE**  
**Aggravated Identity Theft**  
**[18 U.S.C. § 1028A]**

22. Count Nine incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

23. On or about May 14, 2015, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and**  
**FREDRICK BROWN (2)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, and social security number, belonging to H.C., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT TEN**  
**Aggravated Identity Theft**  
**[18 U.S.C. § 1028A]**

24. Count Ten incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

25. Between on or about October 19, 2016 and December 20, 2016, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and**  
**JONGMIN SEOK (5)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, bank account number, and Veterans Administration file number, belonging to A.D., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT ELEVEN**  
**Aggravated Identity Theft**  
**[18 U.S.C. § 1028A]**

26. Count Eleven incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

27. On or about March 6, 2017, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and**  
**JONGMIN SEOK (5)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Department of Defense identification number, belonging to R.W, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT TWELVE**  
**Aggravated Identity Theft**  
**[18 U.S.C. § 1028A]**

28. Count Twelve incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

29. On or about March 9, 2017, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1),**  
**FREDRICK BROWN (2),**  
**ALLAN ALBERT KERR (4), and**  
**JONGMIN SEOK (5)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Department of Defense identification number, belonging to F.C., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT THIRTEEN**  
**Aggravated Identity Theft**  
**[18 U.S.C. § 1028A]**

30. Count Thirteen incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

31. On or about October 10, 2017, in the Western District of Texas and elsewhere, the Defendants,



**ROBERT WAYNE BOLING, JR. (1), and  
ALLAN ALBERT KERR (4)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name, date of birth, social security number, and Veterans Administration file number, belonging to L.W., during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**COUNT FOURTEEN  
Aggravated Identity Theft  
[18 U.S.C. § 1028A]**

32. Count Fourteen incorporates by reference, as if fully set forth herein, paragraphs one through fifteen of this Indictment.

33. On or about June 18, 2018, in the Western District of Texas and elsewhere, the Defendants,

**ROBERT WAYNE BOLING, JR. (1), and  
TRORICE CRAWFORD (3)**

did knowingly use, and aid, abet, induce, and procure the use of, without lawful authority, a means of identification of another person, to wit, a name and bank account number belonging to E.R, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely Conspiracy to Commit Wire Fraud, as charged in Count One of this Indictment, knowing that the means of identification belonged to another actual person.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

**NOTICE OF GOVERNMENT'S DEMAND FOR FORFEITURE**

**I. Forfeiture Statutes for Fraud and Conspiracy**  
**[18 U.S.C. § 981(a)(1)(C), as made applicable by 28 U.S.C. § 2461(c)]**

As a result of the foregoing criminal violations set forth in Counts One through Seven, the United States gives notice that it intends to forfeit, but is not limited to, the property listed below from Defendants **ROBERT WAYNE BOLING, JR., JR. (1), FREDRICK BROWN (2), TRORICE CRAWFORD (3), ALLAN ALBERT KERR (4), and JONGMIN SEOK (5)**. The Defendants shall forfeit all right, title, and interest in said property to the United States pursuant to FED. R. CRIM. P. 32.2 and 18 U.S.C. § 981(a)(1)(C), which is made applicable to criminal forfeiture by 28 U.S.C. § 2461(c). In pertinent part, Section 981 provides:

**18 U.S.C. § 981. Civil Forfeiture**

**(a)(1)** The following property is subject to forfeiture to the United States:

\* \* \*

**(C)** Any property, real or personal, which constitutes or is derived from proceeds traceable to . . . any offense constituting "specified unlawful activity" (as defined in section 1956(c)(7) of this title), or a conspiracy to commit such offense.

Wire Fraud is an offense constituting "specified unlawful activity" as defined in section 1956(c)(7) of this title.

**II. Forfeiture Statute for Money Laundering**

**[18 U.S.C. § 982(a)(1)]**

As a result of the foregoing criminal violations set forth in Count Eight, the United States gives notice that it intends to forfeit, but is not limited to, the property listed below from Defendants **ROBERT WAYNE BOLING, JR. (1), FREDRICK BROWN (2), TRORICE CRAWFORD (3), ALLAN ALBERT KERR (4), and JONGMIN SEOK (5)**. The Defendants shall forfeit all right, title, and interest in said property to the United States pursuant to FED. R. CRIM. P. 32.2 and 18 U.S.C. § 982(a)(1), which states:

**18 U.S.C. § 982. Criminal Forfeiture**

(a)(1) The court, in imposing sentence on a person convicted of an offense in violation of section 1956, 1957, or 1960 of this title, shall order that the person forfeit to the United States any property, real or personal, involved in such offense, or any property traceable to such property.

**III. Subject Property**

This Notice of Demand for Forfeiture includes, but is not limited, to the following:

**Money Judgment:**

A sum of money that represents the property involved in and/or the amount of proceeds traceable, directly or indirectly, to the violations set forth in Counts One through Eight for which each Defendant is liable.

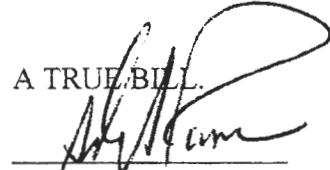
**Substitute Assets:**

If any of the property described above, as a result of any act or omission of Defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

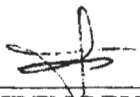
it is the intent of the United States to seek the forfeiture of any other property owned by Defendants up to the value of said Money Judgment as substitute assets, pursuant to FED. R. CRIM. P. 32.2 and 21 U.S.C. § 853(p).

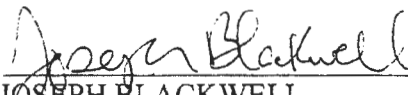
A TRUE BILL.

  
FOREPERSON

GUSTAV W. EYLER  
Director, Consumer Protection Branch  
United States Department of Justice

JOHN F. BASH  
United States Attorney

By:   
EHREN REYNOLDS  
YOLANDA MCCRAY JONES  
Trial Attorneys

By:   
JOSEPH BLACKWELL  
Assistant United States Attorney